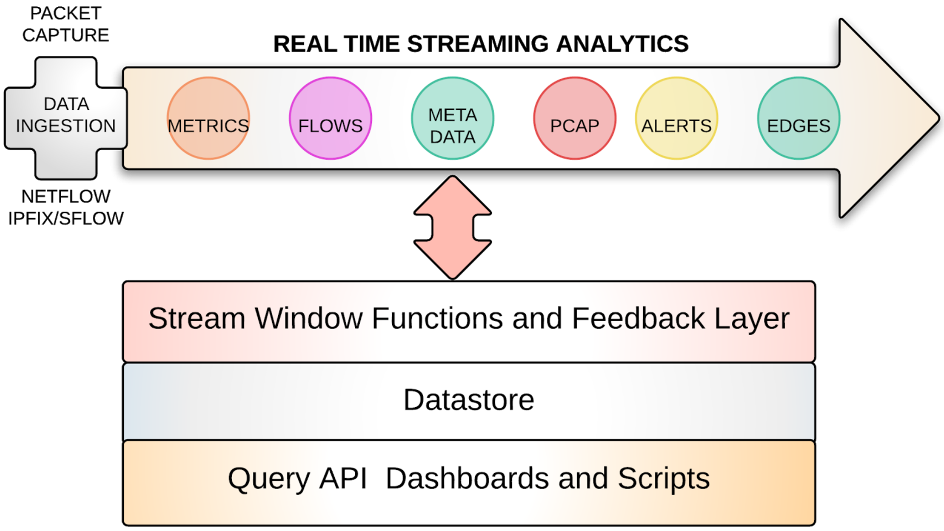
TRISUL Trisul Network Analytics 6.5

Network Security Monitoring & Traffic Analytics Platform

DATA SHEET FOR PACKET BASED ANALYTICS

Trisul Network Analytics 6.5 enables organizations to deploy comprehensive network visibility, network security monitoring, threat hunting, and incident response capabilities. Trisul works with **FULL PACKET CAPTURE** or **NETFLOW** technologies to provide real time visibility and historical analytics. Trisul uses streaming analytics algorithms to give you real time results rather than the traditional search or database backed solutions. The image below shows the six building blocks of Trisul : Traffic Metrics, Network Flows, Metadata, Security Alerts, and raw Packet storage. The latest Release 6.5 features EDGE - a fast streaming graph analytics subsystem for exploring relationships..


PACKET CAPTURE
REAL TIME STREAMING ANALYTICS
DATA INGESTION
METRICS
FLOWS
META DATA
PCAP
ALERTS
EDGES
NETFLOW IPFIX/SFLOW
Stream Window Functions and Feedback Layer
Datastore
Query API Dashboards and Scripts

Traffic and Bandwidth Metrics : In-Depth Visibility is the bedrock

Trisul brings best-in-class visibility to your network traffic. While processing raw packets it continuously extracts over 200+ traffic metrics at high resolution (as fine as 100 msec) without any roll ups or summarizations for long term time-series analytics. Advanced statistical metrics like cardinality counters (eg unique applications per host) and top-N snapshots are all enabled out of the box. You can create your own custom metrics using our simple API. A few of the 200+ metrics include Hosts, Applications, Ports, Countries, AS Numbers, MAC, VLAN, Layer-2 Metrics, SSL Orgs, Certificates, Ciphers, HTTP Response codes, Social Media traffic profiles, URL category, etc. **Real Time Stabbers** allow you to bring up a 1-sec real time view of any metric. This allows for fast troubleshooting.

Flow analysis : Highly scalable flow database for investigation

A flow represents an IP conversation. Trisul reconstructs flows from packets, indexes them, and stores them in a custom built database designed to scale to billions of flows with sub-second query response time. The **Explore Flows** tool allow you to query the flow database using any criteria. Trisul features a streaming algorithm called a **Flow Tracker** that snapshots various interesting flows such as Elephant Flows, Suspicious Flows, Large Payload Transfers out of your network, etc. All flows are stored without roll ups for lossless security investigations.

Metadata : Extracts objects from network traffic

Trisul extracts various types of *objects* from packet streams. They are stored as **Resources** and as **Full Text Search FTS Documents.** Some example are DNS records, HTTP URLs, SSL Certificates, File Hashes, Reconstructed Binary files, and full HTTP header logs. These can be queried during investigation or to scan them for indicators of compromise.

Security Analytics: Integrate with IDS and Threat Intelligence systems

Trisul interfaces with popular IDS (Intrusion Detection Systems) and processes the alerts through the same streaming analytics pipeline. This allows tight correlation between intrusion alerts and other data types in Trisul. For example you can **Flow Tag** all flows that generate a

Priority-1 alert and then query for that later. Trisul includes a plugin called **Badfellas** that automatically pulls down carefully curated open threat intelligence feeds and scans your traffic against them. **Real Time Alert Stabber** is a powerful real time alert dashboard that you can leave on a large screen display.

Packet Analytics : Dive down into packet level from any context

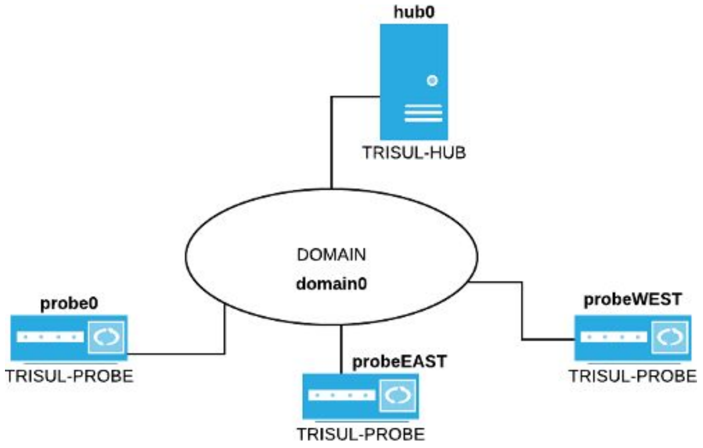
Trisul indexes and stores all packets in an encrypted format. Dive down to packets from Flows, Alerts, Traffic Spikes, or from any compromise time interval. Powerful per-flow pruning policies allow you to skip unnecessary traffic from being stored thereby boosting your retention interval. Furthermore you can use simple LUA Scripts to apply your business rules to further prune what gets stored and how much.

Extensibility : Simple Lua yet powerful

The Trisul LuaJIT API allows you to integrate your own detection and metrics into the Trisul Streaming Analytics engine. Your team is no longer dependent on a vendor to build your own tooling. The **Trisul Apps GitHub** repository is a growing library of extensions using this API.

DISTRIBUTED ARCHITECTURE

Trisul Network Analytics can be used in a Hub and Probe configuration. The Hub provides the database and reporting function. The Probes do the packet capture, streaming analytics. Packets are stored remotely on the probe while other data types make it to the Hub Node. **Contexts** allow multiple network monitoring tenants. A single monitoring domain can have multiple isolated *contexts* sharing the same infrastructure. This allows MSPs and enterprises to monitor disjoint networks without mixing up the data



Trisul NSM vs IPS vs IDS

Trisul Network Analytics	Intrusion Prevention System	Intrusion Detection System
Passive - does not block traffic	Inline - blocks traffic	Passive
Historical storage	Limited, focused on blocking	-
Deep visibility Traffic Metrics	-	-
Flow reconstruction and storage	-	-
Database included	No DB. Export to 3rd party	No DB
Category of Network Management System	Category of Network Device	Category of Network Device
Use Case: Visibility,, Security, Analytics, Alerting,Incident Response, Audit, and Compliance	Use Case: Protection, Firewall role, Attack detection like DoS, Throughput.	Use Case : Detection, Performance, Signature quality, forwarding alerts to SIEM, Splunk, Elastic.

TYPICAL SYSTEM REQUIREMENTS

< 300Mbps	< 1Gbps	10Gbps+
Single Probe+Hub	Single Probe+Hub	One Hub + multiple probes
Core i5 & Above / 16GB RAM/ 1TB HDD/ 1Gigabit NIC for capture / 1Gigabit NIC for management Separate disk 1TB and above for Packet Storage	Xeon 3Ghz+ 12 Core / 16 GB RAM / 2TB HDD /2x1 Gigabit NIC for capture/ 1x1 Gigabit NIC for management Separate 1TB in RAID 0 (striping) for Packet Storage	Hub: Xeon 24 Core /32 GB/ 8TB HDD with INTEL X520/X540 10G Other Capture Vendors also supported. Please contact us. Each Probe : Core Xeon 3Ghz+/8GB/16GB RAM